Modeling, Simulation and Analysis of Public Key Infrastructure

Yuan-Kwei Liu, NASA Ames Research Center, ykliu@mail.arc.nasa.gov
Richard Tuey, Recom Technologies, dtuey@mail.arc.nasa.gov

Abstract

Security is an essential part of network communication. The advances in cryptography have provided solutions to many of the network security requirements. Public Key Infrastructure (PKI) is the foundation of the cryptography applications. The main objective of this research is to design a model to simulate a reliable, scalable, manageable, and high-performance public key infrastructure.

We build a model to simulate the NASA public key infrastructure by using SimProcess and MatLab Software. The simulation is from top level all the way down to the computation needed for encryption, decryption, digital signature, and secure web server. The application of secure web server could be utilized in wireless communications. The results of the simulation are analyzed and confirmed by using queueing theory.

Key Words:
Public Key Infrastructure (PKI), cryptography, queueing model, wireless communication.

1. Introduction

Security is an essential part of network communication. The advances in cryptography have provided solutions to many of the network security requirements, which include:

- Confidentiality: Only the authorized party can read the message.
- Integrity: The receiver must be able to identity that the message has not been tampered with.
- Authentication: The receiver must also be able to confirm that the message is indeed from the right sender.
- Non-repudiation: The sender can not deny that the message was indeed sent by him/her.

The confidentiality, integrity and authentication requirements can be achieved through symmetric key cryptography, which is also called secret key cryptography because the sender and the receiver share the same secret key to encrypt or decrypt a message. The secret key algorithm has high performance, and it has been used widely in the world, such as the Data Encryption Standard (DES).

However, the secret key cryptography has the following shortcomings:

- Key distribution: How do you give the shared key to the other party?
- Digital signature: The sender can deny that she/he sent the message because there is more than one person who knows the key.

2. Public Key Infrastructure

W. Diffie and M. Hellman published a new approach to cryptography in 1976 [1]. R. Rivest, A. Shamir and L. Adleman published the RSA public key cryptography in 1978 [2].

A pair of keys, i.e. a public key and a private key, is used in public key cryptography:

- Encryption/Decryption: Alice uses Bob's public key to encrypt a message and send it to him. Bob uses his private key to decrypt the message.
- Digital signature/Verification: Alice uses her private key to sign a message. Bob uses Alice's public key to verify the signature.

A certificate can be used to bind a person to his/her public key. This certificate is signed by a Certification Authority (CA) to authenticate the public key and its holder. The certificate is normally issued by a Registration Authority (RA) and stored in a directory for lookup and retrieval. A policy is used to enforce the security implementation. The CA, RA, directory, and policy are components of a Public Key Infrastructure (PKI), which is the foundation of many cryptography applications. The certificates used in this model are based on the X.509 standard [3].

3. Modeling of NASA's PKI

The PKI modeling in this paper focuses on the NASA's PKI, which is in the process of being deployed by late 1998. The plan is to establish a Certification Authority at Ames Research Center, and a Registration Authority at Headquarters and each of its field centers. Each field center will have its own directory to store the certificates.

In order to simulate the complete PKI processes, the model is broken into four levels using SimProcess software [4]:

- Level 1 consists of one CA process at Ames Research Center, one RA process at each field center, and a branch activity to direct the certificates back to the originating centers (see Fig. 1).
- Level 2 includes two main functions: registration and applications (see Fig. 2). The applications cover encryption / decryption, digital signature / verification, and secure web server.
- Level 3 models the process in the registration and applications: key generation in Fig. 3, encryption and decryption in Fig. 4, digital signature in Fig. 5, signature verification in Fig. 6, and web guard of secure web server in Fig. 7.
- Level 4 covers the detailed computational sequence of encryption in Fig. 8 and decryption in Fig. 9.

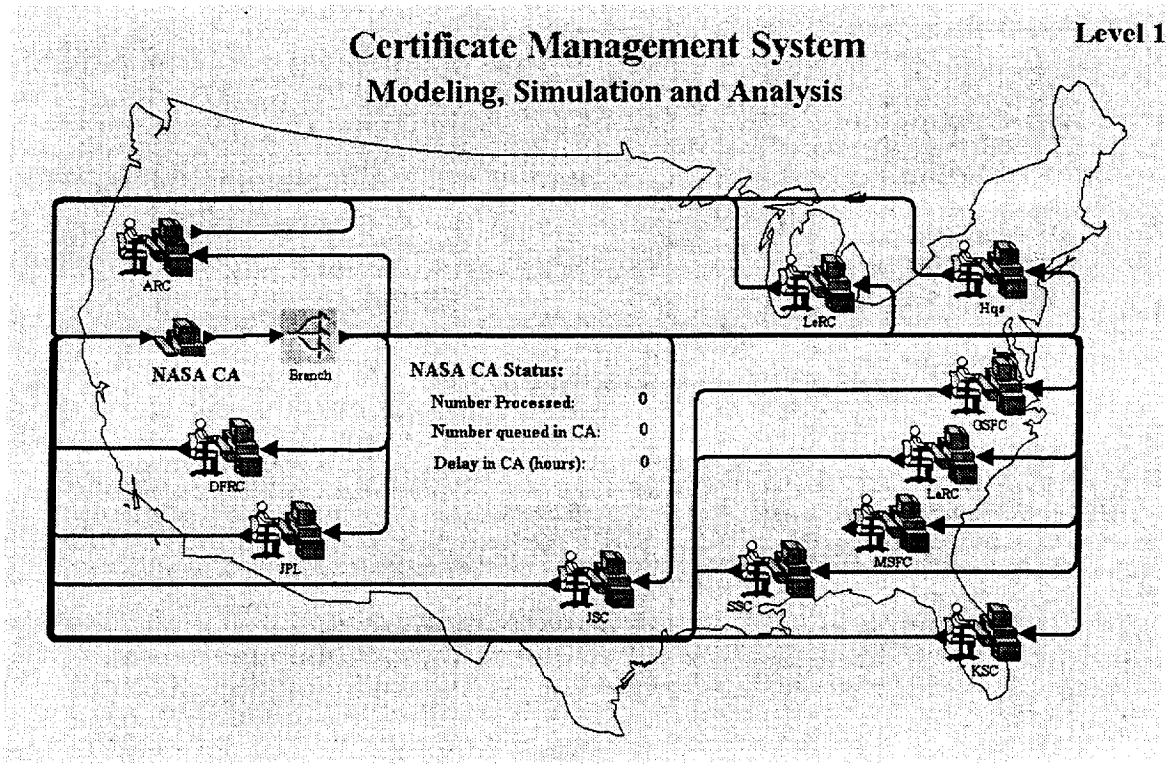

Fig. 1: Level 1 Certificate Management System

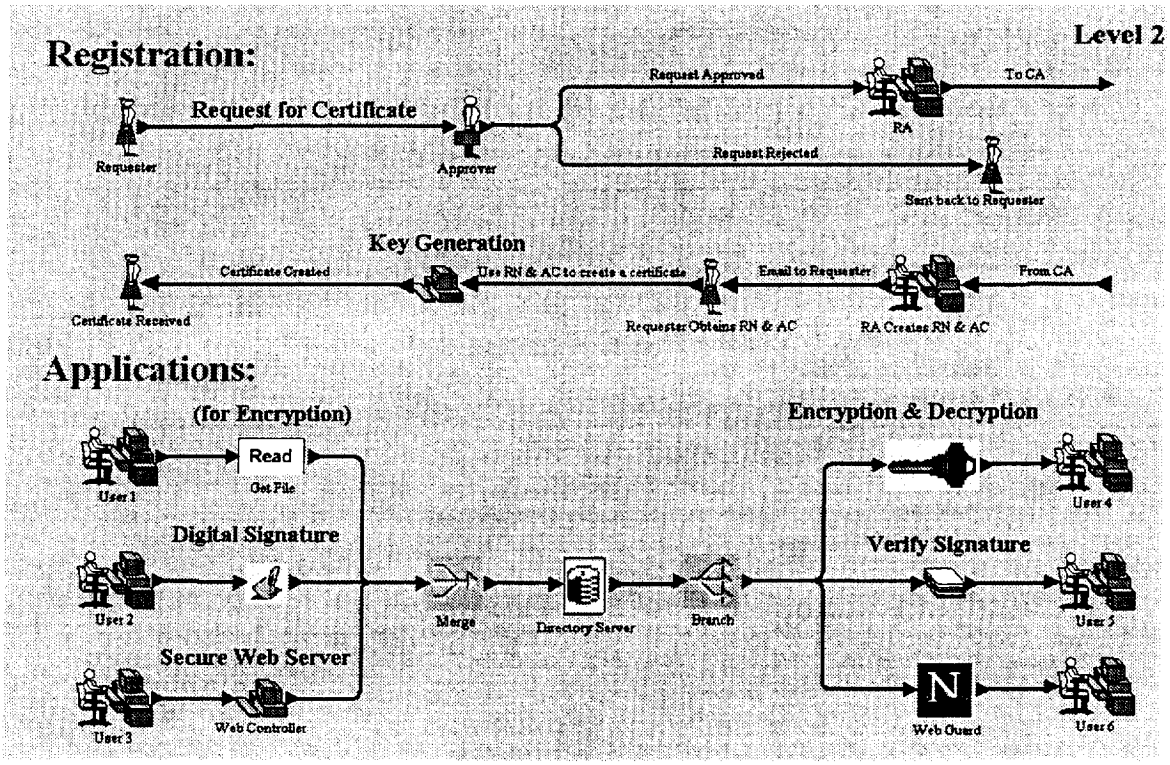

Fig. 2: Level 2 Registration and Applications

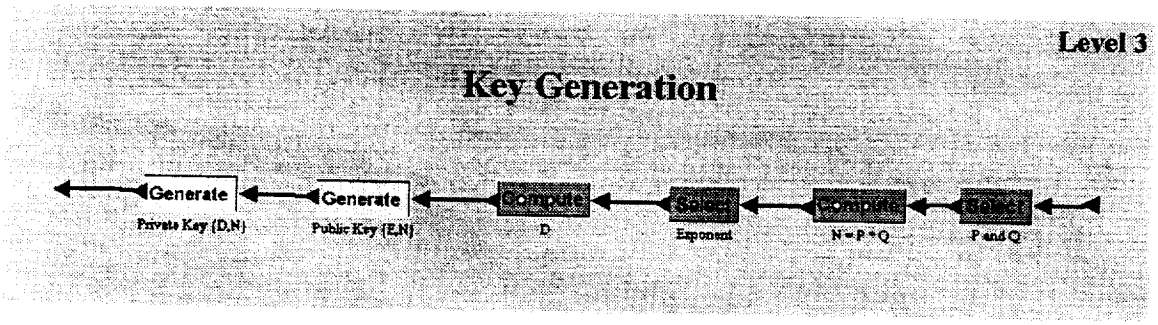

Fig. 3: Level 3 Key Generation

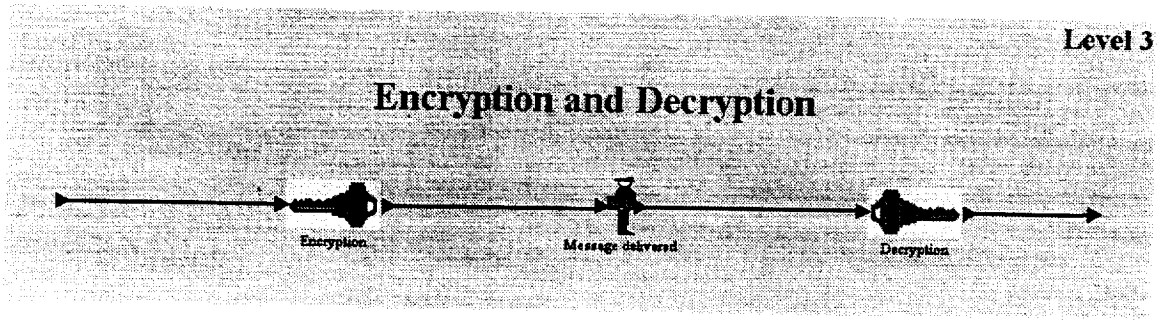

Fig. 4: Level 3 Encryption and Decryption

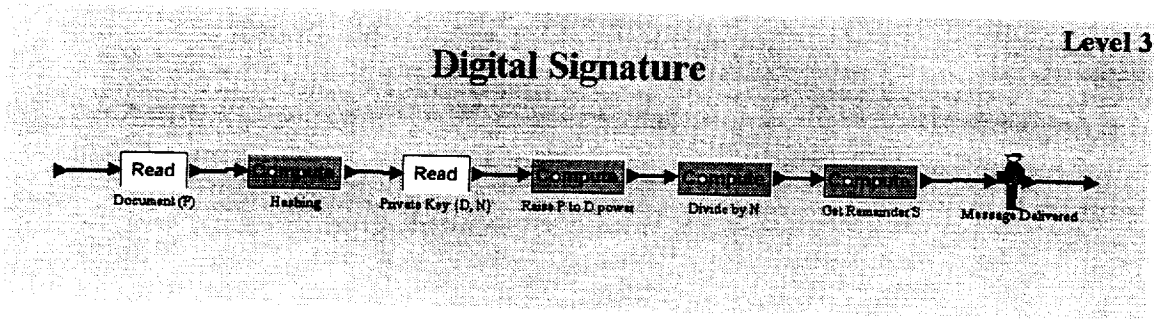

Fig. 5: Level 3 Digital Signature

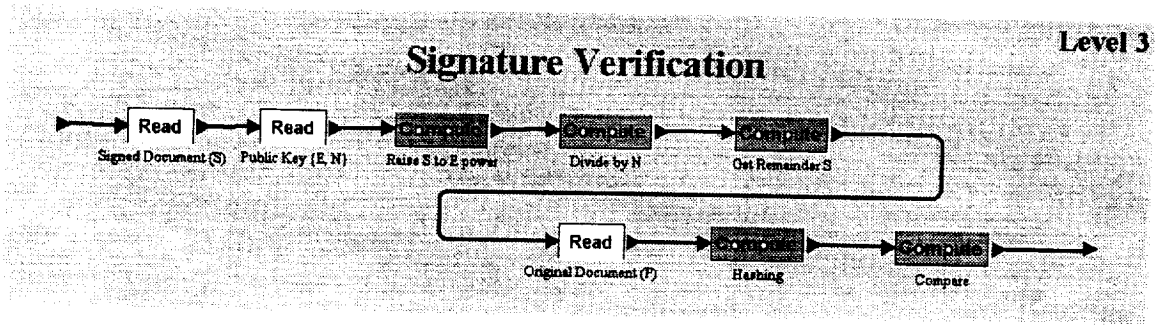

Fig. 6: Level 3 Signature Verification

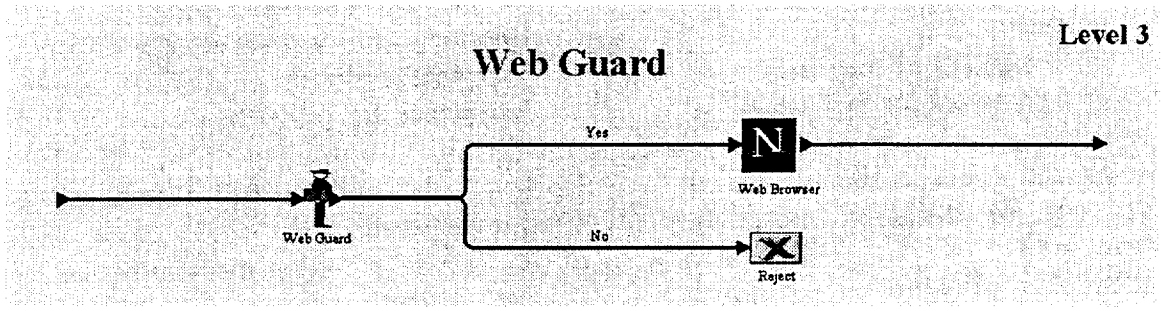

Fig. 7: Level 3 Web Guard

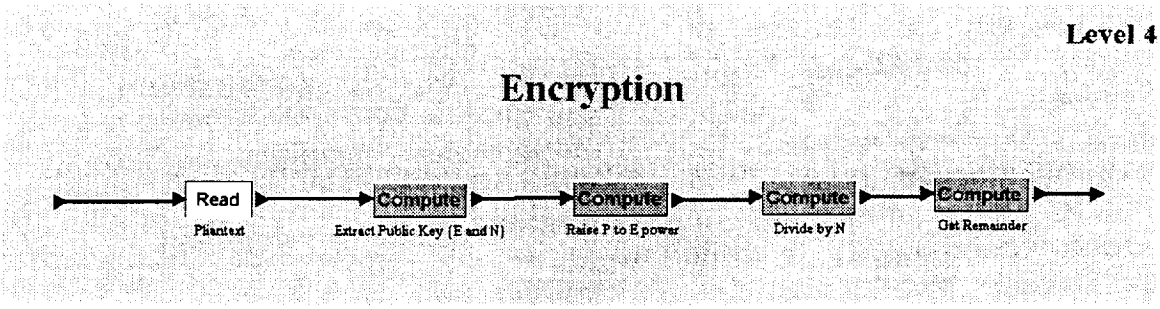

Fig. 8: Level 4 Encryption

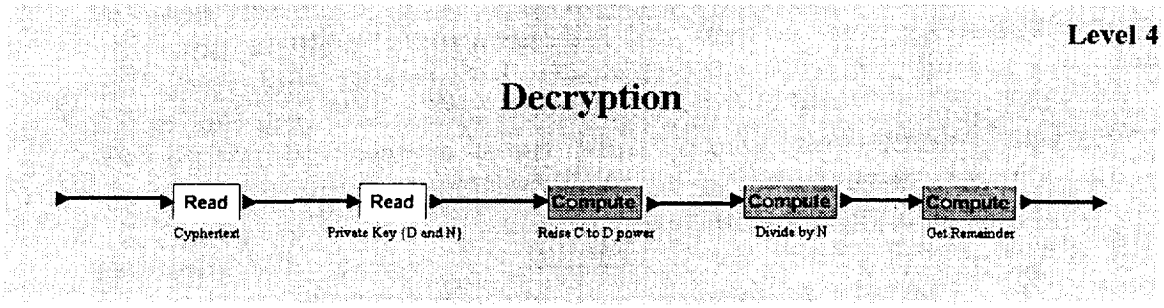

Fig. 9: Level 4 Decryption

4. Secure Web Server and Wireless Communication

The World Wide Web is a powerful communication tool, and the applications of the web have increased dramatically in the past few years. However, some applications may need to control access to certain web pages.

There are two common ways for access control:

- User and password authentication;
- Client hostname and Internet Protocol (IP) address screening.

Using the user and password authentication has several disadvantages:

- The password has to be sent through the communication channel. It may be stolen or reused even though it is encrypted;

- It may be short and easily be guessed;
- Each web server may need to set up a password for each user.

Screening the client hostname and IP address can be done by using the network prefix or the suffix of a hostname. For example, a web server can allow the user with .nasa.gov suffix to access a page. However, it also has several disadvantages:

- The user may not register his IP address in the Domain Name System;
- An IP address may be dynamically assigned using the Point-to-Point Protocol (PPP) provided by an Internet service provider, or using the Dynamic Host Configuration Protocol (DHCP);
- There are no mechanisms to securely and automatically update a domain name server at the present time.

The security issue could be even more serious for wireless communication, which is increasing in popularity. The traditional analog cellular phones are very insecure. The 32-bit serial number, the 34-bit telephone number, and the conversation in a cell can be "scanned" easily by an all-band receiver. The widely used AMPS (Advanced Mobil Phone System) is an analog cellular phone system. Therefore, sending a password or a hostname through this system can be a serious security issue.

Another security issue in wireless communication is in communication satellites, which has many advantages over wired communication:

- Mobil communication;
- A message can be broadcasted to thousands of receivers at once;
- No hostile terrain, or right of way problems, etc.

However, the broadcasting feature of satellite communication could cause a major security problem: everybody can receive every message. Therefore, cryptography is essential for wireless communication when security is required.

As far as web access control is concerned, an alternative solution is to use a public key certificate, along with a web controller and a web guard program.

When a user wants to access a page, he can use his private key to sign a request for access. The request is sent to a web controller. The controller uses the requester's public key in the directory to verify his signature and checks the access control list. If both are verified, the controller then informs the web guard to authorize the web access.

Signing a request by using the requester's private key, without sending any confidential information, provides protection in wireless communication.

5. Simulation and Analysis of Registration Process

The simulation includes two processes: the registration process and the application process.

The registration process has a server (i.e. NASA CA as shown in Fig. 1) and thousands of certificate requesters from each center. This process can be represented as an M/M/1 queueing

model with Poisson arrivals, exponential (Markovian) service times, and the number of servers is one.

In this M/M/1 model, the service rate (μ) which is the computer speed of Certification Authority, is much higher than the interarrival rate (λ) which is the human speed of Registration Authority. Therefore, even though there is only one CA creating certificates for the whole NASA community, the server utilization rate ($\rho = \lambda/\mu$) will be very low and there is no performance problem.

6. Simulation and Analysis of Application Process

The application process, shown in Fig. 2, can also be represented as a M/M/1 model. In each NASA center, there is a directory server that stores user certificates for applications to retrieve the user's public key. The access time to a directory could be different when (1) the certificate is found in the local directory server; (2) the certificate is found in another center's directory server; (3) the certificate is not found at all.

The assumed mean interarrival time is 3 seconds/arrival and the mean service time is 2 seconds/arrival.

The SimProcess simulation was executed and the results are shown in Table 1 with the following notations:
Lq: the number of arrivals in the queue,
Ls: the number of arrivals in the system,
Wq: the waiting time in the queue,
Ws: the waiting time in the system, and
ρ: the server utilization rate

	SimProcess	MatLab	Theoretical
Lq	*	1.35	1.33
Ls	1.93 sec.	2.01	2.00
Wq	3.83 sec.	4.01	4.00
Ws	5.83 sec.	5.98	6.00
ρ	66.08 %	66.49	66.67

Table 1: Results of an M/M/1 Queue
* Not available in the SimProcess report

In order to verify the correctness of the results, We use another software called MatLab and wrote MatLab programs to verify the results of SimProcess [5]. We then use queueing theory to calculate the theoretical results and compare them with the results from MatLab and SimProcess. The results from SimProcess, MatLab and theoretical calculation are listed in Table 1.

The theoretical results are calculated as follow [6]:

$$Lq = \frac{\rho^2}{1-\rho}$$

$$Ls = \frac{\rho}{1-\rho}$$

$$Wq = 1-\rho$$

$$Ws = \frac{1}{\mu} + Wq$$

Where $\rho = \lambda / \mu = (1/3) / (1/2) = 0.6667$.

The curves of Ls and Ws versus ρ for the M/M/1 queue in Fig. 10 and 11 show the relationship between these variables [7]. As the directory server utilization rate, ρ, increases and approaches 1, the number of arrivals in the system, Ls, and the average waiting time in the system, Ws, approach infinity.

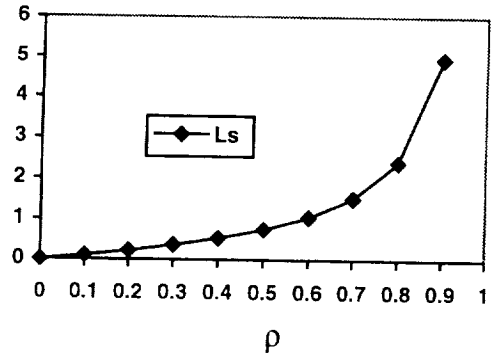

Fig. 10: Ls vs. ρ for an M/M/1 Queue

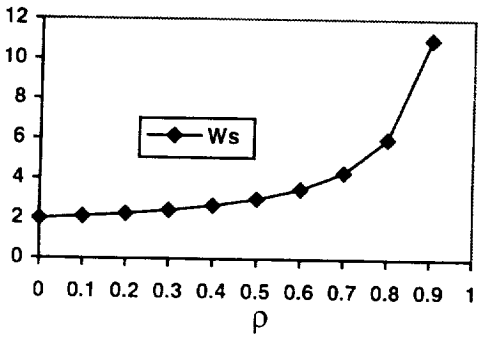

Fig. 11: Ws vs. ρ for an M/M/1 Queue

There are three applications shown in Fig. 2: encryption/decryption, digital signature and secure web server. The number of applications will increase as more and more applications use certificates.

There are three applications shown in Fig. 2: encryption/decryption, digital signature and secure web server. The number of applications will increase as more and more applications use certificates.

In the future, when the number of users and the number applications increase, the only directory server in each center may be a performance bottleneck when ρ approaches 1.

In addition, if the directory server fails, the PKI is down. The single point of failure and the reliability problem could be a serious issue.

If a directory server can only serve up to a certain number of users, the scalability of PKI could also be a problem.

One way to solve the above problems is to increase the service rate, μ. However, we still have the reliability and scalability problems.

The other way is to increase the number of directory servers, c. In this case, we'll have an M/M/c queueing model.

7. Lessons Learned in Simulating an M/M/3 Queueing Model

A MatLab program is implemented to simulate an M/M/3 queueing model with three servers. The assumed average interarrival rate is 3 arrival/second and the average service rate is 1.2 arrival/second.

It is an interesting learning experience to write MatLab programs to simulate the M/M/1 and M/M/3 queues because every detail in the queueing process have to be considered. For example, the expected number of arrivals in the queue, Lq, can be calculated as the total integrated area of the queue duration time divide by the total duration time. The first ten pieces of integrated area is listed in Table 2. The number in front of the multiplication is the number of arrivals in the queue, and the two numbers inside the parentheses are the time periods when this number of arrivals is waiting in the queue.

Number	Integrated Areas
1	1 * (4.792163 - 4.754428)
2	2 * (4.920536 - 4.792163)
3	1 * (5.434270 - 4.920536)
4	0 * (5.565315 - 5.434270)
5	1 * (5.721122 - 5.565315)
6	0 * (5.745093 - 5.721122)
7	1 * (5.827488 - 5.745093)
8	2 * (5.927124 - 5.827488)
9	1 * (5.947090 - 5.927124)
10	0 * (6.359555 - 5.947090)

Table 2: Ten Pieces of Queue Duration Time

A SimProcess program is designed to model the M/M/3 queue. The diagram for this model is shown in Fig. 12.

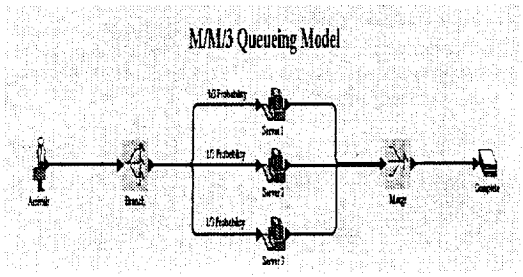

Fig. 12: An M/M/3 Queueing Model

The arrivals are generated at average 1/3 second per arrival. These arrivals are 'branched' into one of the three servers, each has the probability of 1/3 to serve the arrivals. The average service rate is 0.83 second per arrival. A 'merge' activity is provided in order to generate the final results.

The theoretical results are calculated as follow:

$$P_0 = \left[\sum_{n=0}^{c-1}\frac{r^n}{n!} + \frac{cr^c}{c!(c-r)}\right]^{-1}$$

$$Lq = \left[\frac{r^{c+1}/c}{c!(1-r/c)^2}\right]P_0$$

$$Ls = r + Lq$$

$$Wq = \left[\frac{(\lambda/\mu)^c\mu}{(c-1)!(c\mu-\lambda)^2}\right]P_0$$

$$Ws = \frac{1}{\mu} + Wq$$

$$\rho = \frac{\lambda}{c\mu}$$

Where λ is the arrival rate, μ is the service rate, $r = \lambda/\mu$, c is the number of servers and n is the number of arrivals.

The results from MatLab, SimProcess and the theoretical equations are listed in Table 3.

	SimProcess	MatLab	Theoretical
Lq	*	3.49	3.51
Ls	6.47 sec.	5.98	6.01
Wq	1.30 sec.	1.16	1.17
Ws	2.15 sec.	1.99	2.00
ρ	85.08 %	83.33	83.33

Table 3: Results of an M/M/3 Queue

* Not available in the SimProcess report

The reason that the MatLab results are very close to the theoretical results is because the number of arrivals used in the MatLab program was set to high, i.e. 1 million arrivals.

From the above comparisons, the authors are confident that the results generated from SimProcess, which are the simulation program used in this paper, is correct.

8. Conclusion

The results from MatLab, SimProcess and theoretical calculation show that the registration process has no performance issue. The application process may need to increase the number of directory servers when the number of users and applications increase and the server utilization approaches unity.

References

1. W. Diffie and M.E. Hellman, "New Direction in Cryptography," *IEEE Transactions on Information Theory*, v. IT-22, n.6, Nov 1976, pp. 644-654.
2. R.L. Rivest, A. Shamir, and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, v. 21, n. 2, Feb. 1978, pp. 120-126.
3. R. Housley, W. Ford and D. Solo, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile", draft-ietf-pkix-ipki-part1-07.txt, March 25, 1998.
4. SimProcess User's Manual, Release 2.1, 1997, CACI Products Company.
5. MatLab User's Guide, Version 4, 1995, The Math Works, Inc.
6. D. Gross and C. Harris, *Fundamentals of Queueing Theory*, 2nd edition, pp. 58-93, Wiley, 1985.
7. J. L. Hammond and P. O'Reilly, *Performance Analysis of Local Computer Networks*, pp. 81-98, Addison Wesley, 1986.

Appendix: A Sample Decoded X.509 Certificate

```
Version: v3
Serial Number: 832971079
Signature Alg:
md5WithRSAEncryption
(1.2.840.113549.1.1.4)
   Parameters: none
       Issuer: C=US, O=National
Aeronautics and Space
Administration
     Validity: Not Before
960905120642+0800
                 Not After
980905120642+0800
      Subject: C=US, O=National
Aeronautics and Space
Administration, serialNumber=64
+ CN=Yuan K. Liu
SubjectPKInfo: rsaEncryption
(1.2.840.113549.1.1.1)
   Parameters: none
   Public Key:
      modulus:
        00 ba 7f d6 16 db 78 0a
17 26 80 57 2a d7 66 4b
        01 99 de 81 cb 8d 09 95
fb 1a 45 f5 f1 42 62 c3
        62 db ab 6e 9b 33 dd 64
76 bf 02 42 18 d1 39 db
        1d 84 7b de 16 7b 31 c9
ff d7 f2 8b 49 8b 78 9c
        f5
      public exponent:
        03
   Issuer UID: none
  Subject UID: none
   Extensions: 4
  Extension 1: Critical
cRLDistributionPoints (old)
(2.5.29.25)
      SEQUENCE
      . SEQUENCE
      . . SEQUENCE
      . . . SET
      . . . . SEQUENCE
      . . . . . OID
2.5.4.countryName(6)
      . . . . . PrintableString
"US"
      . . . SET
      . . . . SEQUENCE
      . . . . . OID
2.5.4.organizationName(10)
      . . . . . PrintableString
"National Aeronautics and Space
Administra
      tion"
      . . . SET
      . . . . SEQUENCE
```

```
      . . . . . OID
2.5.4.commonName(3)
      . . . . . PrintableString
"CRL1"
  Extension 2: Critical
authorityKeyIdentifier (old)
(2.5.29.1)
      SEQUENCE
      . [0]
      "832970810"
  Extension 3:  keyAttributes
(old) (2.5.29.2)
      SEQUENCE
      . OCTET STRING
      "832971079"
      . [0]
      05 20
  Extension 4:  basicConstraints
(old) (2.5.29.10)
      SEQUENCE
      . BIT STRING number of
bits = 2
      40
Signature Alg:
md5WithRSAEncryption
(1.2.840.113549.1.1.4)
   Parameters: none
Signature Value:
        43 e3 80 04 da 5a 04 4e
26 73 db 90 92 85 c0 1b
        11 ab e2 31 cb b3 fc 61
78 1b 48 15 e1 27 de 0f
        18 f0 38 59 2a e3 01 b1
5d 26 37 2d 88 11 88 25
        4f 04 f7 5b c8 6c dc e1
49 08 44 b4 b0 04 c4 00
        bb 50 a0 ed b2 73 79 f4
35 3f 46 e3 a8 91 32 05
        0c da 93 98 08 37 71 02
4f 08 46 5f 4a 30 98 dc
        d5 6d 56 52 34 3d 54 c9
89 8b f5 39 be d3 f3 fc
        f4 d3 3f aa 7f e0 e9 6d
6f 67 af f0 0b 4e 26 b7
```

IEEE
Networking the World™

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

IEEE Technical Activities Guide

The Technical Activities Guide (TAG) is produced by the IEEE Conference Services Department. This electronic version of TAG is updated daily.

Search

TAG Regions Map

TAG (All Conferences) Sections 1, 2 & 3

Section 1

Section 2
Section 3

TAG By Society

IEEE Aerospace and Electronic Systems
IEEE Antennas and Propagation
IEEE Broadcast Technology
IEEE Computer
IEEE Circuits and Systems
IEEE Consumer Electronics
IEEE Communications
IEEE Components, Packaging, and Manufacturing Technology
IEEE Control Systems
IEEE Dielectrics and Electrical Insulation
IEEE Education
IEEE Electron Devices
IEEE Engineering Management
IEEE Engineering in Medicine and Biology
IEEE Electromagnetic Compatibility
IEEE Geoscience and Remote Sensing
IEEE Industry Applications
IEEE Industrial Electronics
IEEE Instrumentation and Measurement
IEEE Information Theory
IEEE Lasers and Electro-Optics
IEEE Magnetics
IEEE Microwave Theory and Techniques
IEEE Neural Networks
IEEE Nuclear and Plasma Sciences
IEEE Oceanic Engineering
IEEE Professional Communication
IEEE Power Engineering
IEEE Power Electronics
IEEE Reliability
IEEE Robotics and Automation
IEEE Social Implications of Technology
IEEE Systems, Man and Cybernetics
IEEE Signal Processing
IEEE Solid State Circuits
IEEE Ultrasonics, Ferroelectrics, Frequency Control
IEEE Vechicular Technology

TAG Conferences by Region

Region 1
Region 2
Region 3
Region 4
Region 5
Region 6
Region 7
Region 8
Region 9
Region 10

HOME NEWS & INFO IEEE LINKS SEARCH
ABOUT VISITOR'S CENTRE IEEE STORE ONLINE PUBS
[About] [News & Info] [Visitor's Centre] [IEEE Links] [IEEE Store] [Search] [Online Pubs]

Author: IEEE Webmaster (www-societies@ieee.org)
URL: http://www.ieee.org/tag/tag.html

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

IEEE Sponsored, Cosponsored & Topical Conferences
SOCIETY: C
Jun. 01, 1998 - Dec. 31, 2006

*** Revised Listing**
**** New Listing**

TAG NO: 5709
CAT NO: Record

EXHIBIT: Y
ATTENDEES: 300

DATE: Jun. 02, 1998 - Jun. 05, 1998

CONFERENCE NAME:
1998 IEEE 5th International Conference on Software Reuse

INFORMATION CONTACT:
Dr. Ted Biggerstaff
Microsoft Research
One Microsoft Way
Mail Stop 9S/1032
Redmond, WA 98052-6399
(206) 936-5867
(206) 936-0502 (FAX)
tedb@microsoft.com

LOCATION:
Victoria Conference Center
Victoria, BC, Canada

IEEE SPONSORS:
C

OTHER SPONSORS:

TAG NO: 6313
CAT NO: Record

EXHIBIT: N
ATTENDEES: 105

DATE: Jun. 03, 1998 - Jun. 05, 1998

CONFERENCE NAME:
1998 IEEE Real-Time Technology and Applications Symposium

INFORMATION CONTACT:
Professor Raj Rajkumar
Dept. of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
(412) 268-8707
(412) 268-5574 (FAX)
Rag+@cs.cmu.edu

LOCATION:
Executive Tower Inn
Denver, CO

IEEE SPONSORS:

OTHER SPONSORS:

TAG NO: 6216
CAT NO: Record

EXHIBIT: N
ATTENDEES: 80

DATE: Jun. 30, 1998 - Jul. 02, 1998

CONFERENCE NAME:
1998 IEEE Symposium on Computers and Communications (ISCC)

INFORMATION CONTACT:
Dr. Jeffrey E. Wieselthier
Code 5521
Naval Research Lab.
4555 Overlook Ave., SW
Washington, DC 20375
(202) 767-3043
(202) 767-1191 (FAX)
wieselthier@itd.nrl.navy.mil

LOCATION:
Athens, Greece

IEEE SPONSORS:
C
COM

OTHER SPONSORS:

http://www.cs.bu.edu/fta/amass/iscc

TAG NO: 6161
CAT NO: Record

EXHIBIT: N
ATTENDEES: 60

DATE: Jul. 06, 1998 - Jul. 08, 1998

CONFERENCE NAME:
1998 IEEE International On-Line Testing Workshop

INFORMATION CONTACT:
Mr. Matteo Sonza Reorda
Politecnico di Torino
Dauin, Corso Duca degli Abruzzi
24-1-10129, Turin
ITALY
(39) 11 564-7055
(39) 11 564-7099 FAX
sonza@polito.it

LOCATION:
Hotel La Residenza
Capri, Italy

IEEE SPONSORS:
C

OTHER SPONSORS:

TAG NO: 6271
CAT NO: Record

EXHIBIT: N
ATTENDEES: 87

DATE: Jul. 19, 1998 - Jul. 24, 1998

CONFERENCE NAME:
1998 IEEE 6th International Workshop on Modeling, Analysis and Simulation of Computer and Telecommunication Systems

INFORMATION CONTACT:
Mr. Azzedine Boukerche
Simulation Division
Metron #301
Solana Beach, CA 92075
(619) 792-8904
(619) 792-2719 FAX
azedine@cs.mcgill.ca

Sixth International Symposium on Modeling Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'98)

Final Time Table

July 19-20th, 1998

Workshops/Tutorials

Monday July 20th, 1998

18:00-19:30- Registration Open
19:00-21:00 Reception/Welcome

Tuesday July 21st, 1998

8:00	**Registration Open**
8:15-8:30	**Opening/Welcome**
8:30 - 9:30	**Keynote Speaker: Debasis Mitra, Bell Labs, USA**
9:00 - 10:00	**Coffee Break**
10:00 - 12:00	**Paper Session 1**
12:00 - 13:00	**Lunch Break**
13:00 - 15:00	**Paper Session 2**
15:00 - 15:30	**Coffee Break**
15:30 - 17:30	**Paper Session 3**

Wednesday July 22nd, 1998

8:00	**Registration Open**
8:30 - 9:30	**Keynote Speaker: Gregor Bochmann University of Ottawa, Canada**
9:30 - 10:00	**Coffee Break**
10:00 - 12:00	**Paper Session 4**
12:00 - 13:00	**Lunch Break**
13:00 - 15:00	**Paper Session 5**
15:00 - 15:30	**Coffee Break**
15:30 - 17:30	**Paper Session 6**

Thursday July 23rd, 1998

8:00	**Registration Open**
8:30 - 10:00	**Panel Discussion**
10:00 - 10:30	**Coffee Break**
10:30 - 12:30	**Paper Session 7**
12:30 - 13:30	**Lunch Break**
13:30 - 15:30	**Paper Session 8**
15:30 - 16:00	**Coffee Break**
16:00 - 18:00	**Paper Session 9**
19:30 - 21:30	**Dinner (Cruise) at the Saint Laurent River**

Friday July 24th, 1998

8:30 - 10:30	**Paper Session 10**
10:30 - 11:00	**Coffee Break**
11:00 - 12:30	**Tools Track**
12:30 - 13:30	**Lunch Break**
13:30 - 15:30	**Paper Session 11**
15:30	**Close**

- **Last Modified: May, 1998**

Azzedine Boukerche